

Case No. 02AG50553433

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

In re Application of: **MACCHETTI ET AL.**
Serial No.: **Not yet assigned**
Filed: **Herewith**
For: **A METHOD OF IMPLEMENTING ONE-TO-ONE BINARY
FUNCTION AND RELATIVE HARDWARE DEVICE,
ESPECIALLY FOR A RIJNDAEL S-BOX**
Sir:

Transmitted herewith is an INFORMATION DISCLOSURE STATEMENT in the above-identified application.

1. ☒ This IDS is submitted under 37 C.F.R. § 1.97. No fee is required.
2. ☐ This IDS is submitted under 37 C.F.R. § 1.97(c). Enclosed is a check in the amount of \$ 180.00.
3. ☐ This IDS is submitted under 37 C.F.R. § 1.97(c) and (e). No fee is required.
4. ☐ This IDS is submitted under 37 C.F.R. § 1.97(d) and (e). Enclosed is a check in the amount of \$ 130.00 to cover the petition fee.
5. ☒ The Commissioner is hereby authorized to charge or credit any discrepancies in fee amounts to Deposit Account No. 01-0484.
6. ☒ Please associate this application with Customer No. 27975.



27975

PATENT TRADEMARK OFFICE

Date: April 2, 2004


MICHAEL W. TAYLOR
Reg. No. 43,182

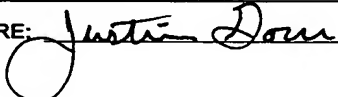
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
MACCHETTI ET AL.

Serial No. **Not yet assigned**

Filing Date: **Herewith**

For: **A METHOD OF IMPLEMENTING ONE-
TO-ONE BINARY FUNCTION AND
RELATIVE HARDWARE DEVICE,
ESPECIALLY FOR A RIJNDAEL S-BOX**

) I HEREBY CERTIFY THIS PAPER OR FEE IS BEING
) DEPOSITED WITH THE U.S. POSTAL SERVICE
) "EXPRESS MAIL POST OFFICE TO ADDRESSEE".
) SERVICE UNDER 37 CFR 1.10 ON THE DATE
) INDICATED BELOW AND IS ADDRESSED TO: MS
) PATENT APPLICATION, PO BOX 1450,
) ALEXANDRIA, VA 22313-1450.
) EXPRESS MAIL NO: EV330385798US
) DATE OF DEPOSIT: April 2, 2004
) NAME: Justin Goree
) SIGNATURE: 


CITATION UNDER 37 CFR §1.97

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

Sir:

Attached is Form PTO-1449 listing several references for consideration in the examination of the above-identified application. A copy of each reference is also enclosed. It is requested that these references be considered by the Examiner and officially made of record in accordance with the provisions of 37 CFR §1.97 and Section 609 of the MPEP.

Respectfully submitted,


MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407/841-2330
Attorney for Applicant

INFORMATION DISCLOSURE STATEMENT			Atty Docket: Serial No.: Applicant: Filing Date: Group:		02AG50553433 Not Yet Assigned MACCHETTI ET AL. Herewith		
U.S. PATENT DOCUMENTS							
Examiner Initials		Document Number	Date	Name	Class	Sub Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
FOREIGN PATENT DOCUMENTS							
		Document Number	Date	Country	Class	Sub Class	Translation
	AI	03/010919	2/6/03	WO	H04L9	06	
	AJ						
	AK						
	AL						
OTHER ART (Including Author, Title, Date, Pertinent Pages, etc.)							
	AM	Ehram et al., Key Controlled Substitution for Cryptographic Applications, March 1978, IBM Technical Disclosure Bulletin, Vol. 20, No. 10, March 1, 1978, Pages 3984-3985, XP002254729					
	AN	Morioka et al., A 10 Gbps Full-AES Crypto Design with a Twisted-BDD S-Box Architecture, Proceedings 2002 IEEE International Conference on Computer Design: VLSI in Computers and Processors, 2002 IEEE International Conference on Computer Design, Freiberg, Germany, September 16-18, 2002, Pages 98-103, XP008021504					
	AO	Morioka et al., An Optimized S-Box Circuit Architecture for Low Power AES Design, Cryptographic Hardware and Embedded Systems - Ches 2002. 4 th International Workshop Revised Papers (Lecture Notes in Computer Science Vol. 2523, Pages 172-186, XP002254730					
	AP	Wolkerstorfer et al., An ASIC Implementation of the AES SBoxes, Topics in Cryptology - CT-RSA 2002. Cryptographers' Track at the RSA Conference 2002. Proceedings (Lecture Notes in Computer Science Vol. 2271), Pages 67-78, XP002254731					
EXAMINER:				DATE CONSIDERED:			

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.